Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

COMMENTS OF T-MOBILE USA, INC.

Josh L. Roland
Michelle Rosenthal
Christopher Koegel

T-Mobile USA, Inc.
601 Pennsylvania Avenue, N.W.
Suite 800
Washington, DC 20004

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

COMMENTS OF T-MOBILE USA, INC.

I. INTRODUCTION AND SUMMARY

T-Mobile USA, Inc. ("T-Mobile")[1] submits these comments in response to the Federal Communications Commission ("Commission" or "FCC") *Notice of Proposed Rulemaking* ("*NPRM*") in the above captioned proceeding.[2] T-Mobile supports the Commission's efforts to make it harder for bad actors to take control of consumers' cell phone accounts through fraudulent subscriber identity module ("SIM") swapping and phone number port-outs. As an industry leader in customer service, T-Mobile has robust protections in place to help prevent fraudulent SIM swapping and port-outs from occurring. If fraud is identified, T-Mobile's teams act swiftly to help customers regain control of their accounts. Targeted FCC rule modifications on number porting and disclosure of customer proprietary network information ("CPNI") will help carriers and third parties deter bad actors and keep wireless users' identities secure.

In considering how to advance its goals in this proceeding, the Commission should recognize that combatting SIM swap and port-out fraud is a team effort that requires action by an entire ecosystem that includes carriers and subscribers as well as financial institutions, email

[1] T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.

[2] *Protecting Consumers from SIM Swap and Port-Out Fraud*, Notice of Proposed Rulemaking, FCC 21-102, Docket No. 21-341 (Sept. 30, 2021) ("*NPRM*").

providers, retail websites, social media companies and others who rely on various customer authentication methods. As the FCC notes, fraudsters sometimes hijack SMS messages to impersonate account owners.[3] Organizations should use authentication measures that correspond to the value and sensitivity of the accounts involved because, while SMS is a useful tool, it was not designed to be used as a method of authentication for third-party accounts.

With respect to the FCC's proposals, T-Mobile supports several changes to the rules. The Commission should adopt its proposal to require reasonable efforts to notify users of port-out requests and SIM changes but preserve carrier flexibility with respect to the method of notification and the time period for processing the requested change. The Commission's rule modifications should not discourage use of one-time PINs ("OTPs") to authenticate port-out requests, nor foreclose other emerging methods of user authentication, particularly given that what constitutes a "secure method of authentication" is likely to change over time. The Commission should also make clear that carriers can offer customers the ability to lock accounts to prevent unauthorized port transfers and SIM swaps, and carriers should have the ability to initiate such locks if high-risk activity is identified. In building in flexibility for carrier response to high-risk activity and unique customer circumstances, the Commission need not specify procedures for carrier response to multiple failed authentication attempts. While multiple failed attempts may be a red flag for fraud, failed attempts can occur for valid reasons and carriers need flexibility to ensure legitimate user needs are met.

At the same time, the Commission should recognize that the vast majority of subscriber SIM swap and port-out requests are legitimate and make sure that any new rules do not keep carriers from honoring valid customer requests. Finally, the Commission should ensure that any

[3] *See NPRM* ¶ 4.

rule changes do not limit consumer choice between wireless providers or stifle competition by introducing undue delay or complexity to fulfilling port-out and SIM swap requests.

II. T-MOBILE USES ROBUST PRACTICES TO DETER FRAUD AND PROTECT CONSUMERS.

T-Mobile uses multi-faceted strategies to avoid the adverse effects that customers can experience as a result of SIM swapping and port-out fraud. T-Mobile has policies in place to combat SIM swap and port-out fraud by empowering customers and deterring malicious actors, including account protection, monitoring, and rapid response to suspected fraud.

Customer Authentication. T-Mobile offers various customer authentication options, which may vary based on customer, account, and device characteristics. T-Mobile customers set up an individual 6-to-15 digit PIN that can be used to verify the customer's identity when calling customer service.[4] As the Commission notes, T-Mobile customers must provide their PIN when requesting a port-out associated with that account.[5] Most customers that choose to create a T-Mobile ID for use on My.T-Mobile.com or with the My T-Mobile app have the option of setting up multi-factor authentication ("MFA") using methods including security questions, SMS, or device-based biometrics such as Face ID or fingerprint recognition on devices that support such features.[6] T-Mobile uses MFA, consistent with the FCC's rules, for validating customer identity and verifying the legitimacy of account changes.

[4] T-Mobile, *T-Mobile Support: Update your Customer PIN/Passcode*, https://www.t-mobile.com/support/account/update-your-customer-pinpasscode (last visited Nov. 8, 2021).

[5] *NPRM* ¶ 53.

[6] T-Mobile, *How T-Mobile Helps Customers Fight Account Takeover Fraud*, (Oct. 29, 2019), https://www.t-mobile.com/news/press/how-to-fight-account-takeover-fraud; T-Mobile, *T-Mobile Support: Set up & manage your T-Mobile ID*, https://www.t-mobile.com/support/account/set-up-and-manage-your-t-mobile-id (last visited Nov. 8, 2021); T-Mobile, *T-Mobile Support: Set up biometric verification*, https://www.t-

T-Mobile's customer authentication methods have evolved in response to identification of vulnerabilities. For example, T-Mobile proactively bolstered authentication practices following release of research associated with the Princeton University study cited by the FCC.[7] The research identified an emerging potential insecurity in using call logs for customer authentication.[8] As noted in the final published paper, T-Mobile subsequently discontinued the use of call logs for customer authentication and notified the researchers.[9] This example highlights how T-Mobile's practices constantly evolve to keep pace with emerging threats.

Account Protection Features. T-Mobile offers customers several options for protecting their accounts. Qualifying customers may wish to enable safeguards such as setting up account takeover protection—a free feature that prohibits unauthorized users from porting the customer's phone line to another wireless carrier.[10] In addition, for most types of customers, T-Mobile can institute a "SIM change block" that helps protect the customer's SIM from being used in other devices. T-Mobile may activate SIM change blocking in cases of high-risk such as where the user has previously been a victim of fraud. As part of these and other continuous efforts to help customers secure their accounts, T-Mobile notifies customers of account changes and requests.

mobile.com/support/account/set-up-biometric-verification (last visited Nov. 8, 2021). Extension of these features to all customers in all brands is part of T-Mobile's ongoing strategy.

[7] *NPRM* ¶ 9 (citing Kevin Lee et. al, *An Empirical Study of Wireless Carrier Authentication for SIM Swaps*, CTR. FOR INFO. TECH. POL'Y, PRINCETON UNIV., at 62, (August 2020) https://www.usenix.org/system/files/soups2020-lee.pdf ("Princeton Study").

[8] Princeton Study at 65 (describing recent numbers (call logs) as an authentication method "that had not been previously tested but we demonstrate is insecure" in the study).

[9] *Id*. at 62 ("In January 2020, T-Mobile informed us that after reviewing our research, it had discontinued the use of call logs for customer authentication.").

[10] *See* T-Mobile, *T-Mobile Support: Account Takeover Protection by T-Mobile*, https://www.t-mobile.com/support/plans-features/account-takeover-protection (last visited Nov. 8, 2021) (this feature is currently offered to most customers and T-Mobile is working on extending it to all customers).

Response if Fraud Occurs. If a customer is a victim of SIM swap or port-out fraud, T-Mobile takes rapid, responsive measures. Customers may report fraud or unauthorized activity by calling T-Mobile's Customer Care hotline, which is available 24/7. When fraud occurs, T-Mobile's Fraud Operations specialists act quickly to ensure all fraudulent changes are corrected and any wrongful T-Mobile account charges are refunded. T-Mobile also assists with phone number recovery and provides victims with documentation of the fraud upon request. For confirmed CPNI breaches, T-Mobile also provides notification consistent with federal law and regulations.

Customer Service Training. T-Mobile trains its employees on how to recognize fraud and account takeover attempts and how to respond if fraud occurs. Customer service representatives complete ongoing interactive training curricula on fraud and response. Moreover, T-Mobile provides resources on combatting fraud to employees. These resources are provided and maintained so that employees are knowledgeable about steps and guidelines for recognizing attack attempts and can properly respond to customer reports of fraud.

Consumer Education. Consumer education is a key part of a holistic approach to security that helps prevent SIM swap and port-out fraud. T-Mobile strives to keep customers informed of best practices for online safety and account protection. T-Mobile publishes Safety Tips to educate subscribers on how to protect themselves online and directs customers to additional resources on identity theft and online safety from the FTC, CTIA, and others.[11] T-

[11] T-Mobile, *Online Safety*, https://www.t-mobile.com/privacy-center/education-and-resources/online-safety (last visited Nov. 8, 2021). *See also* Metro By T-Mobile, *How Metro Helps T-Mobile Customers Fight Account Takeover Fraud*, https://www.metrobyt-mobile.com/simswap.html (last visited Nov. 11, 2021).

Mobile's online resources also inform the customer of what to do if they believe someone has made unauthorized charges to their account.[12]

Ongoing Efforts to Respond to Emerging Threats. T-Mobile engages in ongoing, proactive threat evaluation, and information collection on threats and fraud for internal purposes. For example, T-Mobile gathers and acts on threat intelligence about cybercriminals potentially targeting wireless carriers and customers, conducts penetration tests of our systems, and engages stakeholders to understand emerging attack patterns. Further, as bad actors pivot to new methods and the account takeover fraud landscape changes, T-Mobile implements new strategies to address both known and potential fraud techniques.

Collaborative Efforts. T-Mobile participates in efforts with other stakeholders to address verification issues and stay at the cutting edge of fraud risk management. One such effort was the Mobile Authentication Task Force's Project Verify, which developed the ZenKey mobile authentication platform.[13] T-Mobile's Fraud Prevent product is also evidence of problem-solving across sectors, as T-Mobile partners with financial institutions to provide information that they can use to better authenticate their customers when they are relying on mobile-based authentication. T-Mobile encourages continued industry engagement on verification issues—both within the wireless industry and across the many industries, such as the financial sector, that have need for secure authentication.

III. THE COMMISSION SHOULD NOT IMPEDE CARRIERS' ABILITY TO ACT ON LEGITIMATE SIM SWAP AND PORT-OUT REQUESTS.

T-Mobile's wireless services are a lifeline for its over 100 million postpaid and prepaid subscribers across America, who rely on wireless services for connections to family, work,

[12] *Id.*

[13] *See NPRM* ¶ 54 (discussing ZenKey).

public safety, and school as well as key apps and services.[14] As an industry leader in customer service, T-Mobile supports consumer choice of carrier and device and offers a variety of account and information protections. In considering changes to CPNI and port-out rules, the Commission should strive for rules that (i) enable carriers to meet legitimate customer needs, including the timely accommodation of valid SIM swap and port-out requests, and (ii) promote diversity, inclusion, and accessibility of wireless services.

Wireless services are vital to most Americans and, therefore they must have the ability to make account changes. If devices are lost, stolen, or damaged, and SIM swaps or port-outs are needed, carriers must be able to timely honor legitimate requests and restore access to vital services. Although fraud does occur, legitimate requests make up the vast majority of SIM swap and port-out activity.

The *NPRM* discusses carrier response to multiple failed authentication attempts.[15] It is common for customers to lose or forget their authentication data or have multiple failed authentication attempts. Accordingly, T-Mobile urges the FCC not to mandate specific carrier response to this type of activity such as lengthy "lock out" periods or other severe consequences, which may delay restoration of service. Instead, the Commission should build flexibility into the rules to enable further technology innovations that meet customer evolving needs.

The FCC also asks whether its proposals would pose "particular challenges to customers whose phone associated with their account has been lost, stolen, or destroyed."[16] Indeed, the

[14] *See* T-Mobile US, Inc., SEC Form 10-K for the Year Ended December 31, 2020 (Feb. 23, 2021), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001283699/c2c2789c-74cc-4699-8a9a-34ee1bd9c41e.pdf.

[15] *NPRM* ¶ 33.

[16] *NPRM* ¶ 25.

Commission should consider how changes to its rules would impact various types of users, including prepaid customers. Prepaid service generally does not require identity validation for account set-up. This lack of information may present unique challenges for account protection and recovery when proof of identity is needed. This may require particular flexibility or creativity when a customer has a lost or stolen device and cannot use their SMS to receive an OTP, or for users who may lack access to a back-up device or an online account to receive messages. In addition, while in-person authentication is a useful alternative, it is not always feasible to authenticate an individual for whom the carrier never collected such identifying information, which often is the case in the prepaid context. The Commission should strike the right balance in its rules between deterring fraud and encouraging carriers to support customer choice and provide responsive customer service.

IV. T-MOBILE SUPPORTS CHANGES TO THE COMMISSION'S RULES THAT WILL DETER FRAUD WHILE ENABLING CONSUMER CHOICE AND COMPETITION.

T-Mobile remains vigilant in its efforts to evolve its safeguards to prevent fraud. Accordingly, T-Mobile supports the Commission's efforts to improve customer data security. Several of the FCC's proposed rule changes would help wireless carriers combat SIM swap and port-out fraud. For some of the proposed changes, T-Mobile offers feedback with an eye toward strengthening consumer protections without impeding consumer choice of wireless provider and competition and preserving flexibility to meet the evolving threats to customer security

A. The Commission Should Adopt Rules on User Notification of Port-Out Requests and SIM Changes.

T-Mobile supports the FCC's proposal to require carriers to notify users that a port-out request has been received[17] and its proposal to require carriers to provide customer notification of SIM changes in a timely manner.[18] The Commission need not specify the method of customer notification for port-out or SIM change requests, which should be flexible and reflect customers' preferences. For example, notification could be transmitted to the customer's verified email or via SMS. In addition, the Commission should consider amending its rules to permit carriers to attempt to obtain customer approval (or denial) of the port-out request or SIM change following the notification before taking action, with the understanding that the carrier will proceed with the request if the approval has not been obtained by the end of a certain time period. For example, a notification could be transmitted to a customer notifying them that a port-out request or SIM change has been requested and will automatically be approved within a certain time frame, but noting that the customer may respond to confirm such request is valid and cause the transaction to occur more quickly. Such requirements would help provide increased security for customers.

However, in promulgating a notification requirement, the Commission should not mandate a lengthy delay before a carrier can fulfill a request. The FCC asks whether a 24-hour delay for SIM swap requests while notifying the customer via notification and verification of the request would be appropriate.[19] This is too long. A 24-hour delay could cause hardship for customers with legitimate reasons to request the swap, such as a lost, stolen, or damaged phone.

[17] *NPRM*, App'x A, Proposed rule § 52.37(d).

[18] *Id.* Proposed rule § 64.2010(h).

[19] *See NPRM* ¶ 37.

If the Commission does mandate a delay, it should be configurable by the carriers,[20] and the rules should also provide for the SIM change or port-out request to occur sooner if the customer grants approval in response to the notice. Further, the request should proceed if customer approval has not been received within a particular timeframe. The carrier would attempt to obtain customer approval of the notification within a prescribed time frame, but the carrier would process the request if there were no customer response by the expiration of the time period. Under either scenario, the request should be processed promptly upon customer approval or expiration of the time period for response.

To increase consumer awareness and understanding of account activity, the FCC should also ensure that notifications to users of port-out requests and SIM changes be clear and specific. For example, a user notification for a port-out could read: "A port-out from [carrier] to [carrier] was requested for [###-###-####]. Reply with a 'Yes' or 'No' to proceed with your port-out request." Notifications should also include a timeline for response and provide further instructions if the account change is unauthorized. The exact language should be customizable by the carrier to account for the type of request, brand, product, and other factors.

B. The Commission Should Support Carrier Use of a One-Time PIN for Port-Out Requests.

Another tool for validating port-out requests is an OTP. Use of an OTP for port-out requests offers additional security benefits beyond those provided by passcodes. Consumers tend to rely on easily guessable or phish-able PINs and reuse them across multiple accounts. This

[20] The ability to configure the period of delay would give carriers flexibility to address different levels of risk. Varied factors may lead a carrier to delay action or to move more quickly; for example, a SIM change that occurs at 2 AM local time for the user or a SIM change that occurs only a few days after a recent SIM activation on a new device might warrant a longer delay than other types of requests.

makes PINs vulnerable to bad actors with access to prior breach dumps or who engage in social engineering. Use of an OTP for port-outs avoids these vulnerabilities.

The Commission's proposed rules should reflect the benefits of OTPs and encourage (but not require) carrier use of OTPs for validating port-out requests. To this end, the Commission should revise the proposed language of § 52.37 to recognize that a "passcode" could be an account passcode or an OTP to be verified in connection with a port-out request. In addition, the Commission should not require that a passcode or PIN be "requested and assigned by the end user,"[21] as OTPs may not fit this definition. A rigid requirement to use an OTP is not advisable, as secure methods of authentication and carrier practices may evolve over time.

C. The Commission Should Allow Carriers to Offer Consumers the Option to Lock Their Accounts to Prohibit Unauthorized Port-Outs.

T-Mobile supports the Commission's proposal to modify its port-out rules to enable providers to "offer customers the option to lock their accounts to prohibit unauthorized port requests."[22] T-Mobile already offers this functionality to most customers.   Carriers also should not be prevented from offering customers the option of disabling SIM changes to their accounts that are requested by telephone and/or online access.

In addition, the FCC should explicitly authorize carriers to proactively place port-out blocks on accounts in high-risk situations. There may be instances where the carrier notices unusual activity and can act before fraud occurs to aid customers in securing their accounts. Customers would be notified that the port-out block has been instituted on their accounts. To avoid competitive abuse of this feature, the FCC could define "high-risk" to include scenarios involving subscribers (including enterprise customers) whose accounts were previously

[21] *NPRM*, App'x A, Proposed rule § 52.37(c).

[22] *Id.*, Proposed rule § 52.37(e).

compromised in a port-out attack or in a data breach. These changes would help carriers do their parts in assisting consumers with account security.

D. The Commission Should Recognize that Legitimate Users May Make Failed Authentication Attempts, and Not Mandate Particular Procedures for Failed Attempts.

The Commission asks several questions about how carriers handle failed authentication attempts, and whether new regulations are needed.[23] Failed authentication attempts may signal nefarious activity but also occur with regularity for legitimate users. Moreover, tracking failed authorization attempts can be challenging. Users may attempt to access their accounts in numerous ways (*e.g.*, over the phone, via online chat, in carrier stores, in third party retailer stores). Carriers need flexibility to respond to failed authentication attempts that may occur for valid reasons. Consistent with its proposed rule,[24] the Commission should not mandate specific procedures for carrier response to failed authentication attempts. Further, if the FCC adopts its proposal to require wireless carriers to "develop, maintain, and implement procedures for responding to multiple failed authentication attempts,"[25] the FCC should provide a reasonable timeline for compliance so that carriers can implement new policies without disrupting existing operations.

E. Flexible Standards for Authentication Will Promote Innovation in Security.

The Commission discusses various methods of authentication from the traditional (*e.g.*, showing photo identification in-store) to emerging (*e.g.*, blockchain).[26] The FCC should continue to give carriers flexibility to offer various secure methods of customer authentication.

[23] *See, e.g.*, *NPRM* ¶ 33.

[24] *NPRM*, App'x A, Proposed rule § 64.2010(f).

[25] *Id.*

[26] *See, e.g.*, *NPRM* ¶ 26.

Flexibility will promote innovation and improved security for customers. For example, T-Mobile has been implementing cutting edge authentication tools like use of device-based biometric data verification and Google Authenticator. Carriers should have flexibility to customize authentication measures to address specific customer circumstances. For example, there may be high-risk scenarios where specific or specialized authentication methods can be useful. The FCC should not restrict innovation by locking carriers into an authentication method that may become obsolete or replaced with an improved method in the future.

The Commission should also build in flexibility and room to innovate by rejecting its suggestion to bind carriers to the National Institute of Standards and Technology ("NIST") Digital Identity Guidelines.[27] These guidelines were developed "for federal agencies implementing digital identity services" and, as NIST notes, were "not intended to constrain the development or use of standards outside of this purpose."[28] This document is a good reference for guiding best practices, but not suitable for a compliance tool. It would be inappropriate to require carriers to implement these practices, designed for an altogether different purpose, to address SIM swap and port-out fraud.

F. The Commission Should Build in an Adequate Implementation Period for Any New Rules.

While some of the changes proposed by the FCC can be implemented immediately, others may require a longer implementation timeframe. If new obligations are adopted, the FCC should impose a two-year implementation timeframe. In cases where the FCC is authorizing

[27] *NPRM* ¶ 28 (citing NIST, Department of Commerce, NIST Special Publication 800-63B, Digital Identity Guidelines – Authentication and Lifecyle Management (June 2017; including updates as of March 2, 2020), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf ("NIST Digital Identity Guidelines").

[28] NIST Digital Identity Guidelines at ii.

carriers to offer additional services, such as port-out and SIM change blocks, the rule modifications should take effect more quickly.

V. ALL STAKEHOLDERS SHOULD BE ENCOURAGED TO PROTECT AGAINST SIM SWAP AND PORT-OUT FRAUD USING INNOVATIVE TECHNIQUES.

In addition to the regulatory proposals discussed in the *NPRM*, the Commission should consider whether there are other ways to help prevent SIM swap and port-out fraud. For example, the FCC could coordinate with other regulators, such as financial services or healthcare regulators, on strategies. Other regulators may consider new rules on authentication and steer companies away from relying on methods that are not suitable given the nature and sensitivity of information or functions being accessed. Entities with sensitive consumer information or assets (*e.g.*, financial services, cryptocurrency wallets, healthcare, insurance, etc.) should be encouraged to use appropriate authentication methods that correspond to the sensitivity of accounts or transactions. SMS as the second factor should not necessarily be the sole authentication method. Indeed, that the reliance of financial and cryptocurrency firms on SMS for authentication is driving fraudsters to constantly pursue new avenues of SIM and porting fraud. All stakeholders will need to understand risks and bolster security to deter SIM swap and port-out fraud and its consequences. The Commission should consider engaging in consumer education efforts on ways to protect their online information.

The Commission also may want to coordinate with NIST on addressing authentication issues. It may be timely for NIST to update or relaunch work on the use of SMS in two-factor authentication. SMS as a second factor for authentication may be reasonable if coupled with other verifying information such as location, prior use, or device information. Updated guidance or best practices regarding MFA may be appropriate, particularly for organizations that depend on digital identity, which may need to offer and rely on authentication options that offer greater security than SMS. Taken together, these efforts can help boost the security of users' digital identities and prevent the harmful consequences of fraud.

VI. CONCLUSION

T-Mobile supports the Commission's efforts to combat SIM swap and port-out fraud, and T-Mobile is committed to deterring malicious activity and helping customers regain control of their accounts if fraud occurs. Some of the Commission's proposed rule modifications will further the goals of preventing fraud, and the Commission should remain mindful of the need for carrier flexibility to respond to legitimate customer requests and should not take action that would imperil consumer choice and competition in the wireless industry.

Respectfully submitted,

By: *\/s/*

Josh L. Roland, Senior Director
Michelle Rosenthal, Director
Christopher Koegel, Director

T-Mobile USA, Inc.
601 Pennsylvania Avenue, N.W.
Suite 800
Washington, DC 20004
(202) 654-5900

November 15, 2021